



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
11.03.2009 Bulletin 2009/11

(51) Int Cl.:
H04J 14/02 (2006.01) **H04K 1/02** (2006.01)
H04K 3/00 (2006.01)

(21) Application number: **07017666.4**

(22) Date of filing: **10.09.2007**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK RS

- **Inacio, Pedro Ricardo Morais**
6200-230 Aldeia de Carvalho (PT)
- **Monteiro, Paulo**
3930-209 Ilhavo (PT)
- **Morais, Rui**
2795-048 Linda-a-Velha (PT)

(71) Applicant: **Nokia Siemens Networks Oy**
02610 Espoo (FI)

(74) Representative: **Bruglachner, Thomas E.**
Nokia Siemens Networks GmbH & Co. KG
Patentabteilung
Postfach 80 17 60
81617 München (DE)

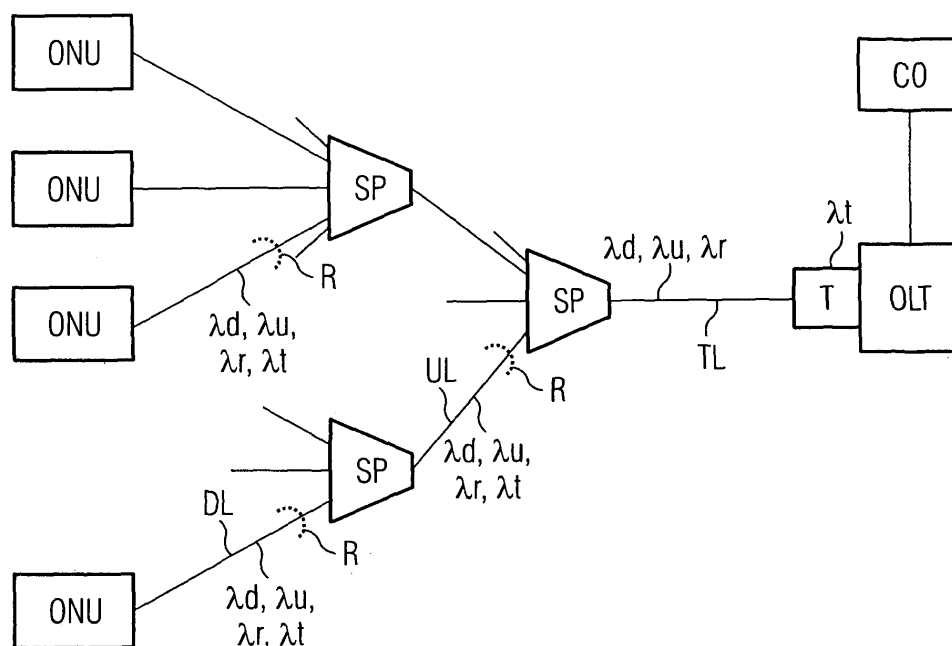
(72) Inventors:
• **Hajduczenia, Marek**
4505-314 Fiaes (PT)

(54) **Method to secure the upstream data transmission in an optical network**

(57) The invention is related to A method to secure a confidential data transmission in the upstream direction of a point-to-multipoint optical network of optical lines, on which the data is transmitted upstream and downstream in different wavelength ranges (λ_d , λ_u), said optical network comprising an optical line terminal (OLT), at least

one splitter (SP) and multiple optical network units (ONU), **characterized in that** an additional disturbing signal (λ_t) is emitted downstream with a wavelength in the range of the upstream data transmission which superimposes with unwanted downstream reflections (λ_r) of the upstream data transmission.

FIG 1



Description

[0001] The invention is related to a method to secure a confidential data transmission in the upstream direction of a point-to-multipoint optical network of optical lines, on which the data is transmitted upstream and downstream in different wavelength ranges, said optical network comprising an optical line terminal, at least one splitter and multiple optical network units.

[0002] Passive optical networks are low cost access networks that provide means to deliver telecommunication signals from a central office via an Optical Line Terminal OLT to subscribers near Optical Network Units ONU. The direction from the central office to the subscribers is called downstream while the reverse direction is called upstream. Since a single OLT is connected to several ONUs through a complete passive optical infrastructure, the downstream communication is of the point-to-multipoint type, which means that all ONUs connected to the OLT receive the same signal emitted by the OLT. Upstream communication is of the point to point type, as all signals from the ONUs are merely combined together in the splitters. This requires channel sharing, which is usually done by a time division multiplexing mechanism.

[0003] To secure the downstream data transmission usually data encryption mechanisms are used, thus only the ONU with the correct key has the capability to decrypt the received packets and extract useful information. On the other hand, the upstream communication is assumed to be secure due to its point-to-point properties and thus no additional security means are currently applied there. Nevertheless, security can be an issue since there can occur unwanted spurious reflections at optical connections in the upstream direction leading to a security threat.

[0004] In principle, the ONU receiver is tuned to the downstream transmission wavelength. However, a malicious user may easily prepare an ONU to detect signals transmitted at the upstream wavelength. So a malicious user may be capable of eavesdropping upstream communications originating from other ONUs in the network by detecting the unwanted reflections of the upstream signal in downstream direction.

[0005] Privacy and confidentiality might be lost if the network operation relies on assumed upstream signal security properties.

[0006] Downstream data signal encryption, preventing eavesdropping by other ONUs, is significantly easier to implement providing that the upstream channel is immune to eavesdropping. In the case of a non-secure upstream channel, the key exchange mechanisms required need to be inherently more complicated. This leads to overhead and undesired consumption of processing capacity and consequently to more expensive equipment.

[0007] In the international patent application WO 2005/032024 A1 a method and system for secure upstream transmission in optical networks is described, which aims to solve the problem of unwanted signal reflections. This application proposes to place disturbing

reflectors along the upstream channel in order to deliberately produce reflections. The combination of the produced reflections with the unwanted reflections of the upstream signal can make it impossible to decode the upstream data signal by any malicious ONU. This method requires reflectors to be distributed along the optical lines, which will be expensive and requires the intervention of highly skilled technicians. Additionally, a malicious user can locate the disturbing reflectors by sending, for example, a short pulse in the upstream direction and detecting its reflections. With this information the mentioned user can try to decode the obtainable upstream signal reflections through a correlation process, providing that the interference between individual reflections is not coherent.

[0008] It is the objective of this invention to solve the above mentioned problems and to propose a secure upstream data transmission without additional equipment in the splitters or at the optical lines.

[0009] This is achieved by the method of claim 1 and the network features of claim 9.

[0010] Embodiments of the invention are shown in the dependent claims.

[0011] The proposed method is applied to a point-to-multipoint optical network of optical lines, on which the data is transmitted upstream and downstream in different wavelength ranges. The optical network comprises an optical line terminal OLT, at least one splitter and multiple optical network units ONU. The method uses an additional disturbing signal which is generated at the OLT level and emitted into the downstream direction at a wavelength within the upstream wavelength range, which superimposes with unwanted downstream reflections of the upstream data transmission. The application of a disturbing signal degrades the downstream reflections of the upstream signal to a level where no data can be recovered from the originating noise, regardless of the applied detection means.

[0012] The disturbing signal transmitter may be placed at the OLT or in the optical line to the first splitter. Some types of first splitters have also a parallel input line, at which the disturbing signal may also be placed. These configurations lead to the protection of the whole optical network.

[0013] The disturbing signal optical transmitter can be any optical source, suitable for the required wavelength. Among the possible transmitters is a Light Emitting Diode LED, a Super Luminescent Diode SLD or a semiconductor Optical Amplifier SOA.

[0014] The effect of disturbing the reflected upstream signals can be optimised by tuning the wavelength of the disturbing signal in the upstream range, thus allowing for dynamic adaptation to the particular optical network conditions.

The effect can further be optimised by adjusting the power of the disturbing signal. The disturbing signal reaching each ONU must always be high enough to make signal detection and processing impossible. On the other hand,

the disturbing signal power must always be below the threshold where the lasers of the ONUs become instable. Calculations have shown that in practical networks the output power of the disturbing signal shall be in the range of -7dBm to -22dBm.

[0015] In one execution of the method the disturbing signal is applied continuous.

[0016] In another execution of the method the disturbing signal is applied only during security sensitive network operations, such as network recovery or key exchanging events.

[0017] Additionally, the disturbing signal may carry randomized data sequences.

[0018] The proposed method and network fulfils the objective of securing upstream communications. It adds no proportional cost to the number of network subscribers. The cost of the additional transmitter is shared between all subscribers.

The transmitter can be placed inside the OLT, at the OLT or as a separate module, what ever is convenient.

[0019] This solution eliminates all manual work related to field employment of measures to secure the upstream network communication. The maintenance can be performed remotely and is limited to making sure that the transmitter of the disturbing signal is operating within its tolerance parameters.

[0020] The proposed method can be introduced in already deployed optical networks without the need of physical changes in the network.

[0021] The figures depict the preferred embodiments of the invention.

Fig. 1 shows the network structure.

Fig. 2 shows a part of the network with a separate transmitter.

[0022] In Fig. 1 a typical passive optical network in a tree configuration is shown. It consists of multiple optical network units ONU at the subscriber sites connected to optical splitters and combiners SP via downstream lines DL. The direction to the optical line terminal OLT is connected via the upstream line UL. The first splitter SP is connected via the trunk line TL to the optical line terminal OLT. The network is controlled by the control system CO, which is connected to the optical line terminal OLT.

[0023] The communication is splitted in upstream and downstream data signals in the according wavelengths λ_u and λ_d . These wavelengths do not overlap.

[0024] In some points in the network reflections R of the upstream data signal can occur. This can be at splices, splitters or the like. These reflections produce the unwanted reflected signal λ_r , which can be detected and decoded by a malicious ONU. To prevent this detection and decoding a disturbing signal with the wavelength λ_t in the upstream range is emitted downstream from the transmitter T to all optical network units ONU. This disturbing signal superimposes the reflected upstream sig-

nal λ_r , thus making it impossible to detect and decode the reflected signal λ_r at a malicious ONU.

The transmitter T can be located at the optical line terminal OLT or integrated in it.

[0025] Fig. 2 shows a part of the optical network similar to the network of fig. 1. Here the disturbing signal λ_t is not emitted into the trunk line TL, but the transmitter T uses an additional input line to the first Splitter SP. The reflected signal λ_r from the reflection point R is superimposed in the same way with the disturbing signal λ_t .

References

[0026]

CO	Control System
DL	Downstream Line
OLT	Optical Line Terminal
ONU	Optical Network Unit
R	Reflection
SP	Optical Splitter
TL	Trunk Line
UL	Upstream Line
λ_d	Wavelength Downstream signal
λ_r	Wavelength reflected signal
λ_t	Wavelength disturbing signal
λ_u	Wavelength Upstream signal

Claims

1. A method to secure a confidential data transmission in the upstream direction of a point-to-multipoint optical network of optical lines, on which the data is transmitted upstream and downstream in different wavelength ranges (λ_d , λ_u), said optical network comprising an optical line terminal (OLT), at least one splitter (SP) and multiple optical network units (ONU), **characterized in that** an additional disturbing signal (λ_t) is emitted downstream with a wavelength in the range of the upstream data transmission which superimposes with unwanted downstream reflections (λ_r) of the upstream data transmission.
2. A method according to claim 1, **characterized in that** the wavelength (λ_t) of the disturbing signal is tuneable.
3. A method according to claim 1, **characterized in that** the power of the emitted disturbing signal is adjustable.
4. A method according to claim 1, **characterised in that** the disturbing signal is emitted with a power of -7dBm to -22dBm.
5. A method according to claim 1, **characterized in that** the disturbing signal is applied continuous.

6. A method according to claim 2, **characterized in that** the disturbing signal is applied only during security sensitive network operations.
7. A method according to claim 1, **characterized in that** the disturbing signal is emitted with a constant amplitude. 5
8. A method according to claim 1, **characterized in that** the disturbing signal carries randomized data sequences. 10
9. An optical network of the point-to-multipoint type, on which the data is transmitted upstream and downstream in different wavelength ranges (λ_d , λ_u), said optical network comprising an optical line terminal (OLT), at least one splitter (SP) and multiple optical network units (ONU), **characterized in that** an additional disturbing signal is emitted downstream with a wavelength (λ_t) in the range of the upstream data transmission which superimposes with unwanted downstream reflections of the upstream data transmission to secure the transmission of confidential data in the upstream direction. 15
20
10. A network according to claim 9, **characterized in that** the disturbing signal is emitted by the optical line terminal (OLT). 25
11. A network according to claim 9, **characterized in that** the disturbing signal is emitted by an optical signal transmitter (T) and injected into the optical line from the optical line terminal to the first splitter. 30
12. A network according to claim 9, **characterized in that** the disturbing signal is emitted by an optical signal transmitter (T) and injected into a second optical input line from of the first splitter (SP). 35
13. A network according to claim 9, **characterized in that** the optical signal transmitter (T) is a light emitting diode, a super luminescent diode or a semiconductor optical amplifier. 40

45

50

55

FIG 1

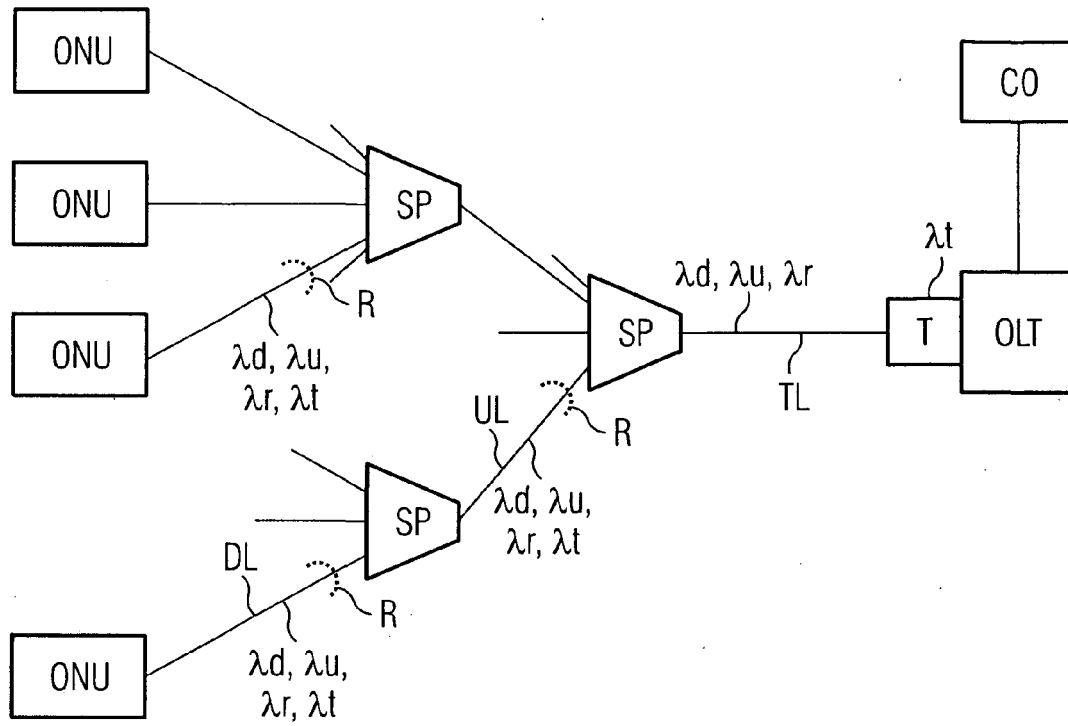
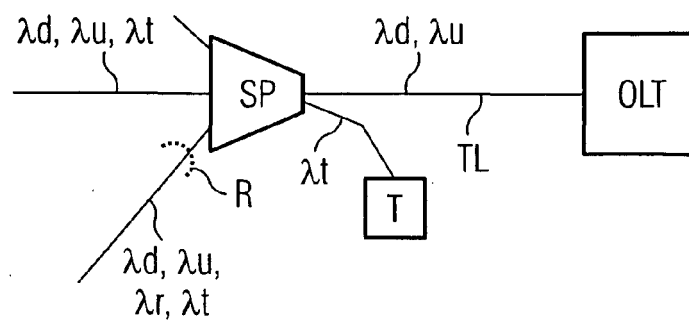


FIG 2





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 01 7666

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	WO 00/30281 A (TELCORDIA TECH INC [US]) 25 May 2000 (2000-05-25) * page 1, line 10 - page 4, line 11; figures 1,2 * * page 5, line 5 - page 7, line 11; figures 5-7 * * page 8, line 1 - line 4 * -----	1-13	INV. H04J14/02 H04K1/02 H04K3/00
A,D	WO 2005/032024 A (NOKIA CORP [FI]) 7 April 2005 (2005-04-07) * page 1, line 7 - line 11 * * page 1, line 32 - page 4, line 16; figures 1,2 * * page 7, line 32 - page 11, line 23; figure 3 * -----	1-13	
A	ROBERT D FELDMAN ET AL: "An Evaluation of Architectures Incorporating Wavelength Division Multiplexing for Broad-Band Fiber Access" JOURNAL OF LIGHTWAVE TECHNOLOGY, XX, XX, vol. 16, no. 9, September 1998 (1998-09), XP011029213 ISSN: 0733-8724 * abstract * * page 1549, left-hand column, paragraph 2 * * figure 6 * ----- -/--	1-13	TECHNICAL FIELDS SEARCHED (IPC) H04J H04K H04N
The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of the search 8 February 2008	Examiner ROLDAN ANDRADE, J
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

1
EPO FORM 1503 03.82 (P04C01)



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 01 7666

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	IANNONE P ET AL: "Enhanced Privacy in Broadcast Passive Optical Networks Through the Use of Spectral Slicing in Waveguide Grating Routers" IEEE PHOTONICS TECHNOLOGY LETTERS, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 9, no. 7, July 1997 (1997-07), pages 1044-1046, XP011048792 ISSN: 1041-1135 * abstract * * page 1044, right-hand column, paragraph 2 - page 1045, right-hand column, paragraph 2; figures 1a,1b * -----	1-13	
			TECHNICAL FIELDS SEARCHED (IPC)
The present search report has been drawn up for all claims			
Place of search		Date of completion of the search	Examiner
The Hague		8 February 2008	ROLDAN ANDRADE, J
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

1
EPO FORM 1503 03.82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 07 01 7666

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

08-02-2008

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0030281 A	25-05-2000	US 6404524 B1	11-06-2002
WO 2005032024 A	07-04-2005	CN 1856953 A	01-11-2006
		EP 1668809 A1	14-06-2006
		JP 2007508730 T	05-04-2007
		KR 20060095963 A	05-09-2006
		US 2005074239 A1	07-04-2005

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- WO 2005032024 A1 [0007]